

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
17 February 2005 (17.02.2005)

PCT

(10) International Publication Number  
**WO 2005/015935 A1**

(51) International Patent Classification<sup>7</sup>: **H04Q 7/34**

(21) International Application Number:  
PCT/IE2004/000108

(22) International Filing Date: 9 August 2004 (09.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
2003/0584 7 August 2003 (07.08.2003) IE

(71) Applicant (for all designated States except US): **PER-  
VENIO LIMITED [IE/IE]**; Cronody, Coachford, County  
Cork (IE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **DEAKIN, Ian**  
[GB/IE]; Cronody, Coachford, County Cork (IE).

(74) Agents: **O'BRIEN John, A. et al.**; John A. O'Brien & As-  
sociates, Third Floor, Duncairn House, 14 Carysfort Ave-  
nue, Blackrock, County Dublin (IE).

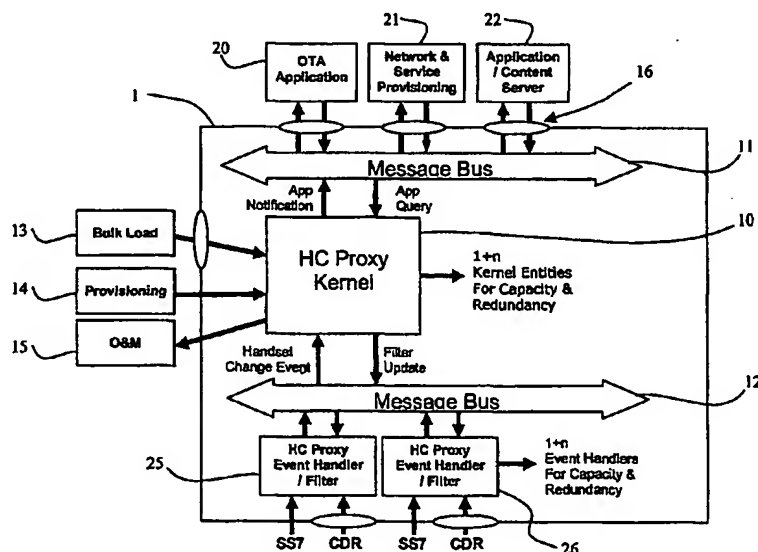
(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,  
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,  
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,  
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,  
ZW.

(84) Designated States (unless otherwise indicated, for every  
kind of regional protection available): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,  
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,  
SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,  
GW, ML, MR, NE, SN, TD, TG).

Published:  
— with international search report

For two-letter codes and other abbreviations, refer to the "Guid-  
ance Notes on Codes and Abbreviations" appearing at the begin-  
ning of each regular issue of the PCT Gazette.

(54) Title: **SERVER FOR DETERMINING AND STORING MOBILE DEVICE CAPABILITY DATA**



(57) Abstract: A handset capability proxy server (1) automatically determines data concerning capabilities of mobile devices and links to users as the devices are used. Event handlers/filters (25, 26) listen to signalling and messaging traffic at different locations in a network. The filter (25, 26) filters out data not relevant to device capability. The handler accesses a RAM cache (37) to dynamically determine if there has been a capability change for a mobile device identifier. It transmits changes to a kernel (10) via a message bus (12). The kernel (10) manages a persistent database (41, 44) of consumer data and device capability data, and automatically notifies subscribed applications in real time.

WO 2005/015935 A1

## SERVER FOR DETERMINING AND STORING MOBILE DEVICE CAPABILITY DATA

INTRODUCTION5 Field of the Invention

The invention relates to mobile networks and mobile devices.

Prior Art Discussion

10

There is a very wide variety of types of mobile devices, each having its own capabilities in terms of service capability, display resolution, colour depth, and multi-media functionality. This creates compatibility problems for content providers and network operators.

15

Mobile application providers and even operators are disadvantaged by the current situation where push applications cannot determine the handset capability. For example, SMS logo graphics and ringtones are very specific to the handset manufacturer and model, and indeed an incorrectly selected ringtone or logo cannot  
20 be detected until the content is received at the handset.

25

Another problem encountered by network operators is non-detection of positive handset churn. When a consumer buys a new mobile device the operator has to enable the appropriate services in the network and the handset must be configured to  
25 connect to these new services.

30

In this specification, the terms "device" and "handset" are used interchangeably. The term "ASP" or "subscribed application" is intended to mean subscribed applications, whereas "consumer" and "user" means a person in possession of a mobile device.

The invention addresses these problems.

SUMMARY OF THE INVENTION

According to the invention, there is provided a mobile device capability server comprising:

5

an input interface for receiving mobile network data in real time;

a processor for automatically determining mobile device capability data from said network data; and

10

an application interface for making said capability data available to applications in real time.

In one embodiment, the network interface listens to network traffic.

15

In one embodiment, the network interface listens to signalling traffic.

In one embodiment, the network interface receives mobile network device authentication data.

20

In one embodiment, the network interface comprises a filter for identifying items of the received network data which is relevant to mobile device capability.

In another embodiment, the filter identifies items of the received network data applicable to a group of users.

25

In one embodiment, the filter identifies items of the received network data by comparisons with a list of users.

30 In one embodiment, the processor comprises at least one event handler for performing initial processing of relevant network data associated with a mobile device.

- 3 -

In one embodiment, the initial processing is event-based, one event being associated with a user and device combination.

5 In a further embodiment, the event handler comprises a cache of existing device capability data linked with users, and the initial processing comprises determining if there is a change in capability of a mobile device of a user.

10 In one embodiment, the processor further comprises a kernel, and a message bus for communication between the kernel and each event handler.

In one embodiment, the event handler transmits mobile device capability change data to the kernel via the message bus, the kernel manages a database of current capability data, and the kernel automatically updates said data upon receipt of said change data.

15 In one embodiment, the kernel transmits the updates to each event handler, and each event handler automatically updates its cache so that all caches and the database are synchronised.

20 In one embodiment, said update is broadcast on the message bus.

In one embodiment, the network interface detects correspondence between a device identifier and a user identifier in one network message.

25 In one embodiment, the network interface receives CDR data transmitted by a network element.

In one embodiment, the network interface receives data from an API of a network element.

30 In another embodiment, the kernel manages a user database and a device database, and automatically maintains links between users and their device capability data.

- 4 -

In one embodiment, the processor automatically notifies subscribed applications of capability changes.

5 In one embodiment, the kernel comprises a rule base of logic for controlling notifications.

In one embodiment, the server further comprises a message bus for communication of capability data between the kernel and the application interface.

10 In one embodiment, the kernel uses the message bus by broadcasting a message onto the message bus, and adapters of the application interface recognise relevant messages.

15 In one embodiment, the adapters recognise relevant messages by listening on particular channels

In one embodiment, the processor tracks usage of different mobile devices by the same user.

20 In one embodiment, the application interface allows user self-provisioning to allow or disallow external application queries.

25 In one embodiment, the processor detects mobile device usage patterns for suspected fraudulent usage, and automatically transmits a message to a network entity if a potentially fraudulent usage pattern is detected.

In one embodiment, the processor allows applications to subscribe to be notified when a specific user changes capabilities.

30 In one embodiment, the processor restricts notifications to data based on pre-configured authorisation properties.

- 5 -

In one embodiment, the processor allows applications to query specific user changes capabilities.

5 In one embodiment, the queries are restricted to data based on pre-configured authorisation properties.

## DETAILED DESCRIPTION OF THE INVENTION

### Brief Description of the Drawings

10

The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only with reference to the accompanying drawings in which:-

15 Fig. 1 is a context diagrammatic representation of a server of the invention and its operating environment;

Fig. 2 is a diagram showing framework of the server;

20 Fig. 3 is a flow diagram for operation of the server to intercept the capability of a mobile device through to the notification of change in capability to applications;

25 Fig. 4 is a flow diagram illustrating how the server detects consumer and handset type identities from a GSM network;

Fig. 5 is a message transfer diagram showing extensions to the GSM MAP messages used by the server to determine handset change;

30 Fig. 6 shows an example of the extended GSM MAP 'Check IMEI' message;

Fig. 7 shows the use of CDR 'Call Detail record' event data by the server to determine handset change;

Fig. 8 shows the use of event feeds directly from a GSM MSC, EIR or HLR by the server to determine handset change;

5 Fig. 9 is a flow diagram illustrating how the server detects downloadable features introducing new capabilities onto a consumer handset;

Fig. 10 is a process flow diagram showing how the server manages flow of information from an observer handset change event, identification of change,  
10 updating the consumer record, and the notification towards external systems;

Fig. 11 is a process flow diagram showing how the server manages subscription by external applications, to be notified about changes on mobile consumers;

15 Fig. 12 is a process flow of the server, showing how the server manages queries from an external application for the current capabilities for a mobile consumer; and

20 Fig. 13 is a process flow of the server operation, showing how the server manages dual SIM cards issued for the same mobile telephone number.

#### Description of the Embodiments

25 Referring to Fig. 1 a server 1 of the invention resides in a mobile network. It communicates with the network infrastructure to detect the presence of a mobile device 2 at authentication. It communicates with core network signalling elements 3 for real time automatic detection of device capabilities. It also communicates with mobile device feature download servers 4 in real time to detect the presence of  
30 additional capability features on the mobile device 2 when they are downloaded onto the device 2. Within the network, it communicates with the mobile operator's operational support services 5 in real time including customer care servers and automatic provisioning servers. It also communicates with external servers 6 for

- 7 -

provision of third party content and applications including direct marketing, ringtone/logo downloading, and games/applications to the mobile devices 2. For device capability queries from servers 5 or 6 it acts as a proxy server, avoiding the need for direct queries to the devices themselves. It may therefore be referred to as a  
5 (handset capability, "HC") proxy server.

The server 1 provides real time device capability notifications to any registered application, for a consumer's handset type and capabilities immediately when the consumer's mobile handset is switched on. This is an un-obtrusive process not  
10 requiring the mobile user to initiate any process or for the device to be constantly polled. The data may be derived from listening to network traffic in real time, or by receiving data from a network element immediately after it is received (e.g. CDR data).

15 Referring to Fig. 2 the server 1 comprises a kernel 10 linked with message buses 11 and 12. It communicates separately from the buses 11 and 12 with bulk load 13, provisioning 14, and O&M 15 servers. The message bus 11 links the kernel 10, via plug-in adapters 16, with an OTA application 20, network and service billing servers 21, and application/content servers 22. The message bus 12 links it with event  
20 handlers/filters 25 and 26. The buses 11 and 12 are separate Java Messaging Service (JMS) buses.

In more detail, the kernel 10 performs the core functions of the server 1 including management of a database of customers, handset profiles, and application profiles. It  
25 executes decision logic to dynamically apply filters to the event handlers and notification of consumer characteristics to ASP applications. It applies the filters by dynamically updating the cache so that it is synchronised with its own database. The kernel database is at the core of the server, maintaining a full inventory of every device on the mobile operator's network including the details of individual device  
30 capabilities for each consumer. The information stored in the database includes:

The phone number (MSISDN) of each handset on the network, with current and list of device types used by this number over a predefined time period.

A list of additional downloaded applications to each handset, beyond the basic features of the manufactured device, i.e. Video Streaming.

- 5 For each phone number (MSISDN) a list of subscribed applications and services which should be notified automatically if the device is changed.

- 10 List of device manufacturer names, models and the list of service capabilities/properties for each, including SMS, WAP, MMS, GPRS, Screen Size, Colour, File formats for Graphics, Music, Video.

A general list of subscribed applications and services which will always be notified automatically by the HC proxy server1 .

- 15 A list of applications which have specific permissions to query capabilities, subscribe/unsubscribe for notification of capabilities on individual consumers.

- 20 Handset movement tracking for fraud detection and consumer behaviour pattern analysis.

Statistical data on handset volumes, usage, churn rates per type accorss the total network.

- 25 The kernel allows a mobile consumer to check through the provisioning interface and check the current settings in the database for their mobile number and display information on applications that have registered to receive information about their capabilities. The consumer can configure their profile to allow or disallow external application query and/or subscribe to receive capability information about their mobile. The configuration of the consumer profile is via a WEB interface.

- 30 The event handler/filters 25 and 26 perform real time, high performance, volume processing of network events which identify handset change by a consumer. This role is to filter and mediate only relevant events, which relate to a handset change.

Essentially, the handlers/filters 25 and 26 non-intrusively listen in real time to signalling traffic and/or call event data at certain network nodes. They filter out non-relevant events and process the relevant data by accessing a cache of last recorded consumer handset data and pass detected changes to the kernel 10 for processing. In this embodiment each handler/filter is capable of handling approximately 25,000 cache-accessing events per second. There is one cache per handler/filter, and it is of c. 2GB RAM size. It therefore allows the server 1 to achieve a high performance. There is a minimum of two handlers/filters, for redundancy.

10

Each handler/filter can be configured to search for only specific groups of consumers to be processed by the server. Examples of these groups are consumers of a particular operator only, roaming-only consumers, specific roaming network consumers or any combination of these groups. This filter is (in GSM) based on the MNC (mobile network code) and MCC (mobile country code) of the consumer IMSI identity.

15

The filter can be configured to search for a specific list of mobile consumer identities or a specific list of device identities. If the filter detects a consumer or device on these lists it sends the events immediately to the kernel 10 for processing. This is used to track consumers and handsets, which have been associated with fraud or required for fault detection.

20

In each handler/filter an event arises for each user-device association detected.

The message bus 12 is also used by the kernel 10 for routing updates to the handlers/filters 25 and 26. These updates are used by the handlers/filters to update the caches. The updates are broadcast by the kernel 10 onto the message bus 12. Each filter listens in on the broadcast to apply updates into the cache.

25

On the other side, the kernel 10 uses the capability data of its database to push notifications to various subscribed application services. This is performed via an application interface comprising the plug-in adapters 16 linked with the message bus 11. The adapters 16 have a common JMS API on the side of the message bus 11, and

30

- 10 -

a particular protocol on the application server side which is compatible with the relevant application server. Each adapter 16 listens on the message buss 11 for a particular channel broadcast by the kernel. There is one adapter for each application, and each adapter is assigned a channel to listen on. There may be multiple adapters  
5 listening on one particular channel, each channel being assigned to a profile rather than to an individual adapter. The kernel 10 includes both pre-configured rules and dynamically provisioned rules based on external application services subscribing to the server 1. Thus, some services are always notified, some are only notified if certain conditions are satisfied, and others are open for a range of applications to subscribe  
10 to.

The server 1 provides open API interfaces to allow integration with the operator network and service entities. The server 1 is scaleable to meet the performance demands of the specific installation and the specific characteristics of the handset  
15 change behaviour from the customer base. Depending on the specific functional demands of the server 1, the server 1 can be easily dimensioned by adding multiple entities to meet the specific requirements.

The adapters 16 provide an ASP (Application Service Provider) interface for the query and distribution of consumer handset capability information. The server 1 can  
20 have multiple instances of adapters for different logical ASP interfaces. Each logical ASP interface can be assigned to an individual external application. The application interface has three main functions:

25       Notifications - this is an asynchronous outbound event interface, providing 1-n number of notifications to the external ASP application. This interface communicates through the message bus 11 and adapters 16.

30       Query - this is a transactional request/response message flow. The ASP can request the capabilities for a given mobile number (in GSM a MSISDN or IMSI). The server 1 provides a response to the request based on the security permissions for the ASP logical interface, the availability of the data for the given mobile number.

Subscribe/Unsubscribe - this is a transactional request/response message flow. The ASP can request the server 1 to register (subscribe) for notifications of consumer's capability change information. The transaction can request one  
5 or a list of given mobile numbers (in GSM a MSISDN or IMSI). The server will provide a response to the request based on the configured security permissions for the ASP logical interface, the availability of the consumer, providing a result code for each individual mobile number in the list. The interface will allow the ASP un-subscribe for notifications of a single or  
10 multiple consumers in the request transaction. The server will respond providing result codes for each individual consumer in the list. Fig. 11 sets out details of the information flow, as described in more detail below.

#### Notification Rules and Subscriptions

15

A server notification rules manager in the kernel 10 defines how and when a notification message or series of notification messages are delivered, to which application provider/service provider they are delivered, and what information is conveyed. The rules can even provide notification messages to a consumer's handset  
20 to prompt them to respond, for example sending an SMS message to the consumer to confirm that this new device is a permanent change, and to check if the consumer would like to be provisioned for the new services associated with this device. The SMS reply sent back by the consumer will be flagged for immediate delivery towards the server 1 so that within a few seconds of the request being sent. The server 1 can  
25 confirm the change and invoke any notifications towards the appropriate services.

A subscription manager in the kernel 10 provides the ability for applications to register to be notified automatically in the event of a handset change by a consumer. Should a mobile operator offer to expose the handset capability, presence and  
30 availability of individual consumers to external Application Service Providers (ASPs), the server 1 can be configured to specify the specific properties for exposing their presence, capability and availability, thus ensuring that they would only present information relevant to authorised applications. The subscription manager will allow

- 12 -

notifications be forwarded for individual phone numbers (In GSM MSISDN numbers) per application type subscribed.

5 The subscription manager provides authentication and authorisation of the applications requesting handset capabilities for a given consumer.

#### Query Management

10 The server 1 performs query management on individual MSISDN numbers. This allows external applications to query the current handset capability from a given consumers MSISDN. A query request is authenticated by the subscription manager and if valid the query manager will check the server database and provide the consumers device capability information to the requesting application. In co-ordination with the subscription rules the information and format of the response is  
15 determined, and then the reply is sent back to the requesting application. Fig. 12 illustrates details of this information flow. The interface for application query is based on an open API standard.

20 The query interface can be used by application to determine the capabilities of handset to format a push application such as SMS ringtone/Logo appropriately.

#### Provisioning and Billing

25 The server 1 is fully configurable across either a WEB or SNMP management interface. Each kernel and event handler process provides operational status and events over an SNMP managenet interface or to a log file viewable via a WEB based application. Any abnormal situations can be alarmed to the operator for investigation.

30 Across the whole server 1 events are generated relating to usage of internal and external resources. These events are passed to a billing system for the purpose of billing settlement reconciliation with external application providers. The operator will then be able to generate interconnect charges for usage based on subscription, Individual query of a consumer and the transportation of notifications.

### Server Process

5

The flow diagram of Fig. 3 illustrates the procedure used by the server 1 to determine the handset capability for a given mobile device.

10

In step 30, the server identifies when the mobile device is switched 'ON', and it initiates an authentication procedure with the mobile network. This is the first thing that happens when a mobile device is switched on and must be completed prior to any other services being available on the mobile device.

15

In real time the server 1 listens to the messages sent by the mobile device and the mobile network when it is switched on, as it performs an authorisation/authentication procedure. These messages can be from the SS7 signalling protocol between the MSC (Mobile switching Centre) and the EIR (Equipment Identity Register)/Equipment Register and or HLR (Home Location Register)/Authentication Server. Alternatively the messages can be directly from the Equipment Registry device or Authentication Server devices through a real time event interface indicating the authorisation/authentication of a mobile device together with the consumer identity and device identity number. The availability of the identities and processing of them is in real time. Fig. 4 illustrates details of the information flow between entities.

25

Examples of alternate sources of the observed consumer identities with the device identity events are given in Figs. 5, 6, 7, and 8.

30

Referring again to Fig. 3, in step 31, the server 1 will immediately process these events of the mobile consumer identity number and the devices equipment Serial number identity to determine the make, model, and capability of the device. One of two procedures will occur at this point.

In step 32, if this consumer's mobile number is already present in the database but has a new device Equipment Serial Number value, then a new additional record is created for this consumer number. The result of a new record being generated for a consumer number will immediately invoke the server 1 to establish the capabilities of the new device for the given mobile number.

In step 33, if the consumer's mobile phone number is new to the server, then a new record is created for this mobile number. If the mobile telephone number (MSISDN) identity of the consumer has to be resolved from an external database the server will perform this.

In step 34, the server 1 is provisioned with a list of manufacturer device capabilities for each handset type. The device Equipment Serial Number of a mobile device includes two specific values important to the determination of the handset type, (A) the first value indicates the manufacturer, (B) the second value indicates the model code. Based on the device Equipment Serial Number provided, the server will determine the device capabilities for a manufacturer and model type. Based on the manufacturer and model, the server 1 will populate the database record for the given consumer mobile phone number with both the text values for the manufacturer/model for example a model including the feature capabilities and properties technical of the handset such as colour screen 150x90 pixels, and MMS, GPRS.

In step 35, once the new record has been created successfully inside the server database, the server will examine the notification rules and will automatically notify any pre-registered application of (A) the consumer mobile number, (B) the new device type and capabilities. The information presented in the notification message can be configured by the server to include all capability details, or only a subset for example colour display, 150X90 pixels. These details in the notification can be different for each registered application. Again this procedure occurs in real time so that applications have knowledge of the change instantaneously the new handset is switched on.

### Device and Consumer Identity Detection

The server 1 collects the data from the mobile network and it uses this data to  
5 identify when a mobile consumer has changed device and subsequently may have  
different capabilities with the new device. The server 1 continuously collects data  
from the mobile network in real time to identify changes in device usage from the  
presence of both the consumer identity and the device identity as soon as it is  
activated. When the mobile device is switched 'ON', the handset will initiate an  
10 authentication procedure with the mobile network, this being standard procedure to  
authenticate and register the mobile device onto the mobile operator network. This is  
the first thing that happens when a device is switched on and must be completed  
prior to any other services being available to a mobile. During this procedure the  
mobile device will present three possible identities, (A) the mobile Phone Number (in  
15 the case of GSM the MSISDN, (B) the mobile device Equipment Serial Number (in  
the case of GSM this is the IMEI number and where a SIM card is used (C) the SIM  
Card identity (in the case of GSM this is the IMSI).

The server 1 can obtain these identities through different methods. Examples of these  
20 methods are described with reference to Figs. 4, 5, 6, 7, and 8.

Referring to Fig. 4, the server 1 connects to the SS7 signalling network to listen to  
signalling information sent and received between the mobile device, the MSC and  
the EIR and HLR during the authentication/registration procedure when the mobile  
25 device is switched on. Based on the Mobile Phone Identity (in the case of GSM the  
MSISDN or IMSI) the Mobile Handset Unique manufacturer serial number (in the  
case of GSM the IMEI. In the case of other networks the ESN.) is captured, and  
recorded.

30 Referring to Fig. 5, the server 1 observes the identities of the device and the  
consumer when the device is switched on and the authentication process of the  
mobile device with the network occurs over the signalling system 7 interfaces. In  
GSM these messages are transferred using MAP (Mobile application Part) protocol.

- 16 -

To enable the server 1 make a connection between the device identity and the consumer identity, both the device and the consumer identities need to exist in one single MAP message. As the standard GSM MAP 'CheckIMEI' message conveys only the device identity, The MAP 'CheckIMEI' message is extended to include the consumer identity. Also the standard GSM MAP 'LocationUpdate' message only contains the consumer identity. The MAP 'LocationUpdate' message is extended in a non GSM standard way, to include the device identity.

Referring to Fig. 6, this indicates the extensions used on the GSM MAP 'CheckIMEI' message so the relationship can be made between the handset IMEI and the consumer identify. In this example the SIM (IMSI) identity is sent with the IMEI.

Referring to Fig. 7, the server 1 connects directly to a billing mediation device, where the CDR 'Call Detail Record' events sent by the MSC (Mobile Switching Centre) for billing purposes are listened to by the server to observe the consumer and device identities. The MSC generates these CDR's events containing very detailed information with respect to usage of and device connecting through it. The mobility management CDRs will contain the customer identity and device identity in a single record. The billing mediation devices are used to groom the data appropriate for billing. In this case the billing mediation can groom the relevant CDR events to be sent to the HC proxy server for detecting device changes.

Referring to Fig. 8, the server 1 can be connected directly with a MSC (Mobile Switching Centre) , EIR (Equipment Identity Register) and/or HLR (Home Location Register) capable of passing programmable API (application programmable Interface) events in real time to the server 1 . These API events include the mobile number (MSISDN or IMSI) and the equipment serial number (In GSM the IMEI. In the case of other networks the ESN.) values for the device being authenticated.

30

Some mobile devices have the ability to download additional feature applications onto the device for the support of WAP, MMS, or media streaming applications. The server 1 can detect the presence and use of downloadable features or mobile

applications, i.e. video streaming application services. The server 1 is able to identify the download of these additional capabilities onto the mobile device, outside of the basic device features. When these new feature capabilities are identified, the server 1 can notify subscribed applications that the consumer now has additional features.

5

Referring to Fig. 9, the server 1 connects directly with download servers to recognise the usage of mobile applications, and applets loaded onto a consumer's device. These servers will send via a programmable API (application programmable interface), events in real time to the server 1 when the download of the application to the device was successful. These API events will include the mobile number (MSISDN) and details of the downloaded application onto the mobile device. Examples of these applications are video streaming applications, multi-media players and device software version updates. These additional capabilities outside of the basic manufacturer's features are recorded to the consumer's record in the server's database.

15

Referring to Fig. 10, the process flow of through the server 1 when used in GSM, from interception of an event containing the device identity with the customer identity and how it is managed through the server. The division between kernel 10 operations and event handler 25, 26 operations is shown by interrupted lines.

20

In a step 36, the event handler checks in the cache 37 for existence of the consumer and if the handset has changed. If the consumer IMSI identity is new (not present in cache 37), then the server 1 sends a request in step 39 to collect the details of this consumer from an external database 42. The consumer telephone number (MSISDN) is resolved from the given IMSI by the server 1. The step 39 sends these two identities together with the device identity to an update process 40 within the kernel 10.

25

If the consumer IMSI identity is present in the cache 37 the event handler will check in step 38 if the handset identity for this consumer is the same. If the device identity is the same, then the server 1 will not proceed from 38 with any actions.

30

- 18 -

If in 38 the consumer IMSI identity is present but the device identity is different to that stored for this consumer identity, then the server 1 will initiate an update process 40.

5 The update process 40 will collect all the historical data from the kernel's "consumer database" 41 for the consumer identity and record the new identities observed. The server 1 compares in step 42 the old and the new device capabilities by comparing the list of capabilities recorded in the device "handset database" 44. The differences in capabilities will be identified in step 45. The list of additional and/or removed  
10 capabilities will be sent to the notification process 46. Based on the logic and the subscription properties listed in a subscription database 47, the process 46 will notify each individual application about the capability changes.

Referring to Fig. 11, this illustrates the process flow of the kernel 10 for an external  
15 application to subscribe to the server 1 to receive notification of the changes in capability for a given consumer's telephone number (In GSM this is MSISDN).

The step 48 receives requests from an external application to subscribe for notifications for a consumer identity. The step 48 will first check the permissions for  
20 this application in the subscription database 47, to check if the request is allowed for this application.

If in step 48 the request is not valid the kernel 10 informs a process 53 of the error code. The process 53 notifies the requesting application that this request was  
25 declined.

If the request is valid, then the kernel 10 notifies an update subscription process 50 to update the subscription database 47 so that this application is recorded to receive the notification data allowed (as detailed in Fig 10. process 46). After Step 50 the  
30 application database is updated successfully. Then step 50 will notify a process 51 to update the consumer record (the identity in the request) that this application must be notified if the capabilities for this consumer change. The process 51 will make an entry in the consumer database 41 on the application identity to be notified.

When the consumer record has been updated then process 51 will send a response code to the inform process 53, which will notify the requesting application that this request was successful.

5

Referring to Fig. 12, this illustrates the process flow of the kernel 10 for an external application to query to the server 1 the current capability for a given consumer telephone number (GSM this is MSISDN).

10 The server 1 receives requests in step 54 from an external application to subscribe for notifications for a consumer identity. The step 54 will first check the permissions for this application in the subscription database 47, to see if the request is allowed for this application.

15 If the request is not valid then the kernel 10 informs a process 58 of the error code and the process 58 notifies the requesting application that this request was declined.

If the request is valid, then the kernel 10 will notify the consumer record process 56 to get the current capabilities for the consumer identity in the consumer database 41.

20 The capabilities of the consumer are passed to the inform process 58, which will respond back to the requesting application.

With SIM-based mobile devices operators can issue multiple SIM cards having individual identities, which share the same mobile telephone number. This will  
25 enable the consumer have more than one handset with its own SIM inside. In this situation it can be possible for two SIMs to be in mobile devices with different capabilities i.e. one SIM and a car phone and another SIM in a PDA. Even though these SIM cards are not exchanged between mobile devices, the HC proxy server 1 can detect the device capabilities for each SIM identity. As each device is switched  
30 on and authenticated with the network, the server 1 will identify the capabilities for each SIM identity. If any differences exist between device capabilities between the multiple SIM cards, the server 1 will notify the subscribed application of the capability changes as the normal process.

Referring to Fig. 13, this illustrates the process flow through the server 1 when used in GSM, for management of dual SIM cards issued for the same mobile number. The division between kernel 10 operations and event handler 25, 26 operations is shown by interrupted lines. In this example the server 1 processes the first SIM card in a first handset event 59. A process 60 of the event handler checks against the identities in this event against the cache 37. As the device or SIM is the same as that in the cache 37 no actions take place. The second device is activated with the second SIM, and this is recognised as an event 65, which is processed in step 60. The step 60 will check these identities against the identities in this event against 61. In this case the customer IMSI is not active and so the step 60 informs an update process 62. The update process 62 will check the consumer record in 41 and will recognise that this is a second SIM for the same telephone number. The update process 62 will inform the cache 37 to implement a step 64 to suspend the current active SIM (IMSI 12345) and to activate the SIM (IMSI 67890) in the cache 37. The process 62 will proceed to notify applications of changes as also described with reference to Fig 10. The first SIM is re-activated with the first device 66 and processed by the step 60. Step 60 checks the identities in the cache 37 and will see that this IMSI is not active. The step 60 will inform the update process 62 and as with the second SIM will update the database 41 and the cache 37 and notifies the applications as in Fig 10.

The server 1 is configured with logic rules to automatically notify applications upon a device type change. These logic rules define which applications should be notified of changes in capabilities, when the server 1 should notify an application of capability changes, how they should be notified and with what information should be sent in the notification. Examples of how the logic rules can be applied to real applications are:

Customer care telemarketing, can be informed only when a new device is used by a consumer that has not changed device in over 1 year.

Automated provisioning systems, GPRS, MMS, WAP, will always be informed when a device is changed. Each system will only receive the information about capabilities, which relate to their service.

5        Automated direct marketing of services, GPRS, MMS, WAP based applications, if a consumer changes capability to enable one of these services for the first time then a message will be sent automatically to the customer welcoming them to the new service.

10       Automatic adaptation of services, when a consumer is using two devices, swapping a SIM between the two. The corresponding services can be automatically adapted as the consumer switched between them.

It is also possible for the server 1 to inform any number of subscribed applications  
15       from ASPs (application service providers) or mobile operator services, that the consumer is now available and can now receive content and if applicable in a new format, based on the capability properties of the new device type, i.e. the ASP can be informed that a consumer subscription for stock notifications is now MMS (Multimedia) including graphs and not SMS text only. This will allow full graphical  
20       displays to be sent to this device.

Mobile marketing messages can be further personalised with content from external servers that is dynamically generated and unique to the consumer who is to receive the message. Before a marketing message is to be pushed to the consumer, the  
25       content server can query the server 1 to determine the capabilities of the device prior to formatting the content, this dynamic content can be included such as a unique bar code or otherwise personalized graphic element formatted correctly to enable it be displayed on the consumers device.

30       This server 1 also eliminates the need for consumers to provision mobile device types. For example, if a user switches to a water proof handset at the weekend for water sports use, these changes can be picked up dynamically and fed back in real

time to the server 1. This ensures that consumers receive the optimal content type relevant to their handset capabilities in real time without any user intervention.

5 The server automatically detects any changes in mobile devices by a user and will automatically expedite events to systems for the purpose of automatic provisioning of any network services compatible with the new device and OTA (over the air) provisioning/configuration of the new handset so that the consumer can access the addition service capabilities of this device i.e. WAP, GPRS, MMS.

10 The server 1 is able to detect a consumer using the same handsets (more than one) over a period of time. The server detects this by maintaining a history of mobile device identities for each consumer. When the server detects that the same set of device identities are being used by the consumer, the server will inform the subscribed systems, services, applications to adapt the service appropriate to the capabilities of the current mobile device being used. The notification to the external  
15 systems to adapt the service for this consumer can be in the form of specific parameters or notification to suspending or enabling the corresponding service.

The server 1 overcomes issues of dual handset/device usage and /or handset  
20 replacement, by being able to provide real time notification to provisioning and applications of the current consumer device capabilities.

The server will furnish any requesting system, service, application or ASP with real time information of the current device capabilities for a given Mobile telephone  
25 number (in the case of GSM the MSISDN number).

The server can determine the capabilities for any mobile device, which is roaming into the network by determining at authentication the identity and the capabilities of the roaming mobile device. When the server detects a roaming device, it will set up a  
30 temporary record in the database for the period that the device is active in the network. The server will notify external applications that this mobile identity is temporary and is roaming from another network. This feature can be used to offer local network service or applications to the roaming mobile for a temporary period.

Also it will enable the local services in the correct format i.e. a welcome message by SMS, MMS, or video.

5 The notification rules of the HC proxy server 1 can be configured to restrict the level of information conveyed in individual notifications of capabilities change to each external system, based on a subscription profile for the requesting system.

10 The server 1 can profile the movements of each individual mobile device on the mobile network identified (by the unique identity of the device) between individual mobile consumers (identified by their mobile number) for the purpose of fraud detection. It maintains a device movement database for each device change to allow alarms to be generated when an individual device movement pattern is associated to fraud. If the server detects a pattern consistent with fraud, it sends a notification to the mobile network HLR to carry out an implicit detach of the mobile device. The  
15 notification will disconnect this device from the network. The server 1 also notifies the HLR to block this consumer from connecting to the network again. The server may also be programmed to track other patterns as required by the network operator and/or the user.

20 The server 1 keeps a constant profile of all mobile devices on the network. This data can be used by a mobile device software update service, which sends software patches/updates to mobile devices. These software updates will be registered in the server 1 database for each device. Therefore if a device is observed on the server 1 which has not received the software update, the software update service can be  
25 informed to send this update to this device.

The real time information provided by the server 1 allows the network operator to dynamically and positively react to customer trends and behaviours from mobile device change by:

30

increased speed of access to new services,

- 24 -

service offering fully compatible with every customers capability, of active device,

increasing revenues from service usage,

5

reducing cost of ownership, and

improving customer satisfaction.

10 The network operator will benefit from the invention through immediate service enabling, maximising content richness and reduced costs from customer care when:

a mobile device is upgraded by a consumer,

15

a mobile device is temporarily upgraded,

there is dual device usage by a consumer, or

an unknown consumer is roaming into the network.

20

Other immediate benefits from this critical real-time information are:

automated provisioning of the mobile operator systems for GPRS, MMS, WAP, with OTA to handset,

25

the operator's customer care, eradication of manual service enabling,

push/Event content applications ringtones, MMS, information services, in the optimal and correct format

30

premium content providers, direct marketing and mobile games / applications.

- 25 -

The server 1 can also inform applications that a consumer is available to receive content in a new more suitable format, to best exploit the properties of the new mobile device.

- 5 The invention is not limited to the embodiments described but may be varied in construction and detail.

Claims

1. A mobile device capability server comprising:
  - 5 an input interface (25,26) for receiving mobile network data in real time;  
  
a processor (10, 25,26) for automatically determining mobile device capability data from said network data; and  
  
10 an application interface (16) for making said capability data available to applications in real time.
2. A server as claimed in claim 1, wherein the network interface listens to network traffic.
- 15 3. A server as claimed in claim 2, wherein the network interface listens to signalling traffic.
4. A server as claimed in any preceding claim, wherein the network interface receives mobile network device authentication data.
- 20 5. A server as claimed in any preceding claim, wherein the network interface comprises a filter (25,26) for identifying items of the received network data which is relevant to mobile device capability.
- 25 6. A server as claimed in claim 5, wherein the filter identifies items of the received network data applicable to a group of users.
7. A server as claimed in claim 5, wherein the filter identifies items of the received network data by comparisons with a list of users.
- 30

- 27 -

8. A server as claimed in claim any preceding claim, wherein the processor comprises at least one event handler for performing initial processing of relevant network data associated with a mobile device.
- 5 9. A server as claimed in claim 8, wherein the initial processing is event-based, one event being associated with a user and device combination.
- 10 10. A server as claimed in claims 8 or 9, wherein the event handler comprises a cache (37) of existing device capability data linked with users, and the initial processing comprises determining if there is a change in capability of a mobile device of a user.
- 15 11. A server as claimed in any of claims 8 to 10, wherein the processor further comprises a kernel (10), and a message bus (12) for communication between the kernel (10) and each event handler (25, 26).
- 20 12. A server as claimed in claim 11, wherein the event handler transmits mobile device capability change data to the kernel (10) via the message bus (12), the kernel manages a database of current capability data, and the kernel automatically updates said data upon receipt of said change data.
- 25 13. A server as claimed in claim 12, wherein the kernel (10) transmits the updates to each event handler (25, 26), and each event handler automatically updates its cache so that all caches and the database are synchronised.
- 30 14. A server as claimed in claim 13, wherein said update is broadcast on the message bus (12).
15. A server as claimed in any preceding claim, wherein the network interface detects correspondence between a device identifier and a user identifier in one network message.

- 28 -

16. A server as claimed in any preceding claim, wherein the network interface receives CDR data transmitted by a network element.
17. A server as claimed in any preceding claim, wherein the network interface receives data from an API of a network element.
18. A server as claimed in any of claims 12 to 17, wherein the kernel (10) manages a user database (41) and a device database (44), and automatically maintains links between users and their device capability data.
19. A server as claimed in any preceding claim, wherein the processor automatically notifies subscribed applications of capability changes.
20. A server as claimed in any of claims 11 to 19, wherein the kernel (10) comprises a rule base of logic for controlling notifications.
21. A server as claimed in claim 20, wherein the server further comprises a message bus (11) for communication of capability data between the kernel (10) and the application interface.
22. A server as claimed in claim 21, wherein the kernel (10) uses the message bus (11) by broadcasting a message onto the message bus, and adapters of the application interface recognise relevant messages.
23. A server as claimed in claim 22, wherein the adapters recognise relevant messages by listening on particular channels
24. A server as claimed in any preceding claim, wherein the processor tracks usage of different mobile devices by the same user.
25. A server as claimed in any preceding claim, wherein the application interface allows user self-provisioning to allow or disallow external application queries.

- 29 -

26. A server as claimed in any preceding claim, wherein the processor detects mobile device usage patterns for suspected fraudulent usage, and automatically transmits a message to a network entity if a potentially fraudulent usage pattern is detected.
- 5 27. A server as claimed in any preceding claim, wherein the processor allows applications to subscribe to be notified when a specific user changes capabilities.
- 10 28. A server as claimed in claim 27, wherein the processor restricts notifications to data based on pre-configured authorisation properties.
29. A server as claimed in any preceding claim, wherein the processor allows applications to query specific user changes capabilities.
- 15 30. A server as claimed in claim 29, wherein the queries are restricted to data based on pre-configured authorisation properties.
31. A mobile device capability server substantially as described with reference to the drawings.
- 20

1/8

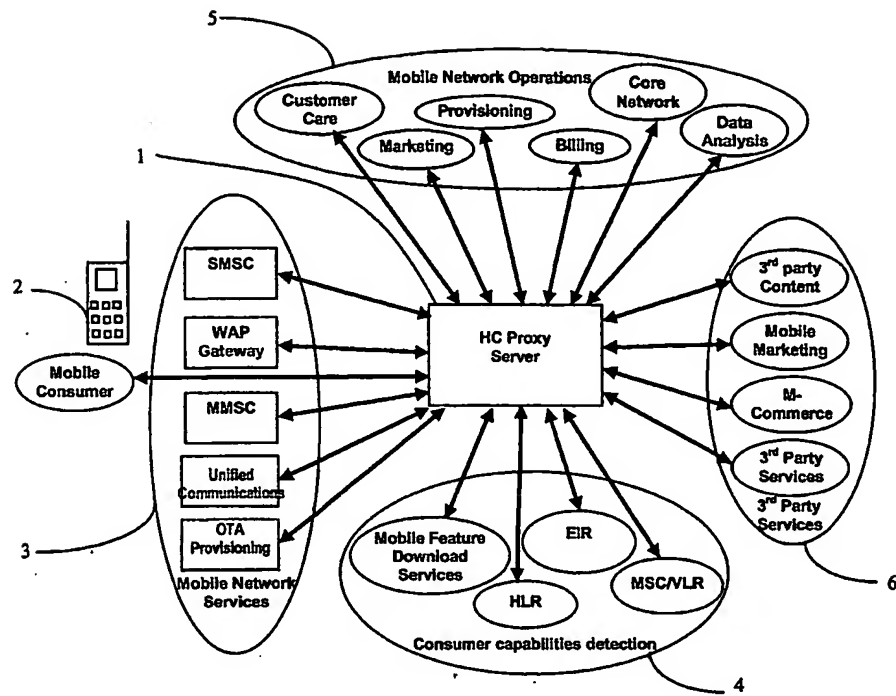


Fig. 1

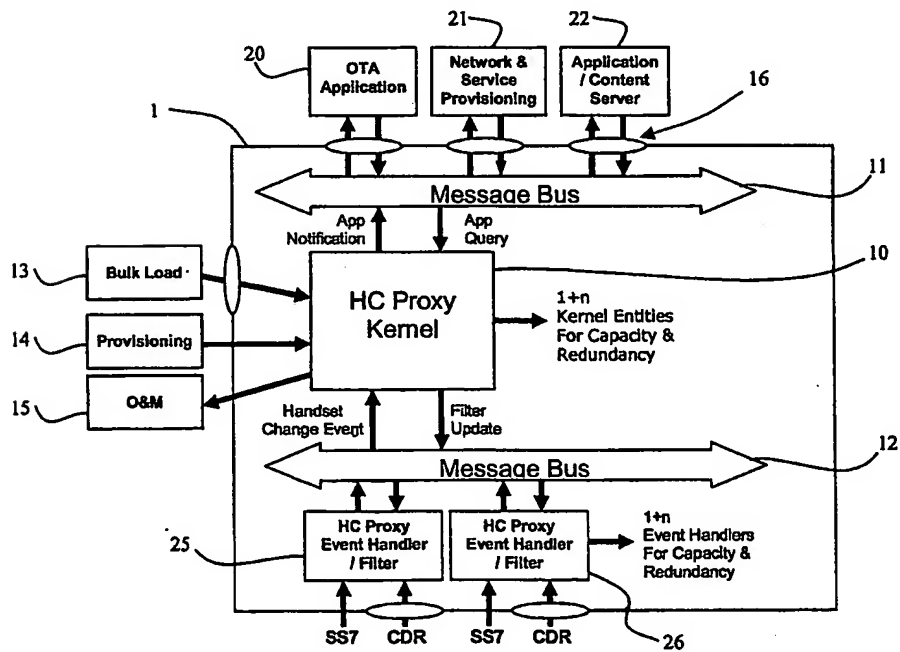


Fig. 2

2/8

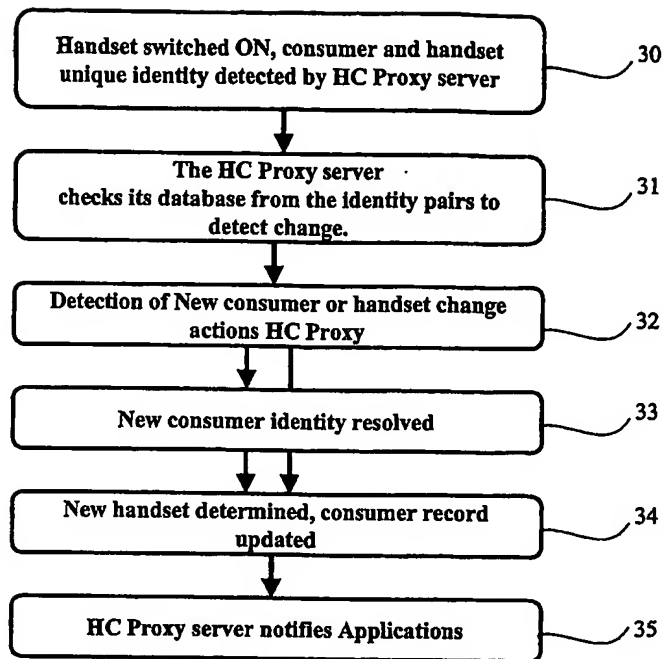


Fig. 3

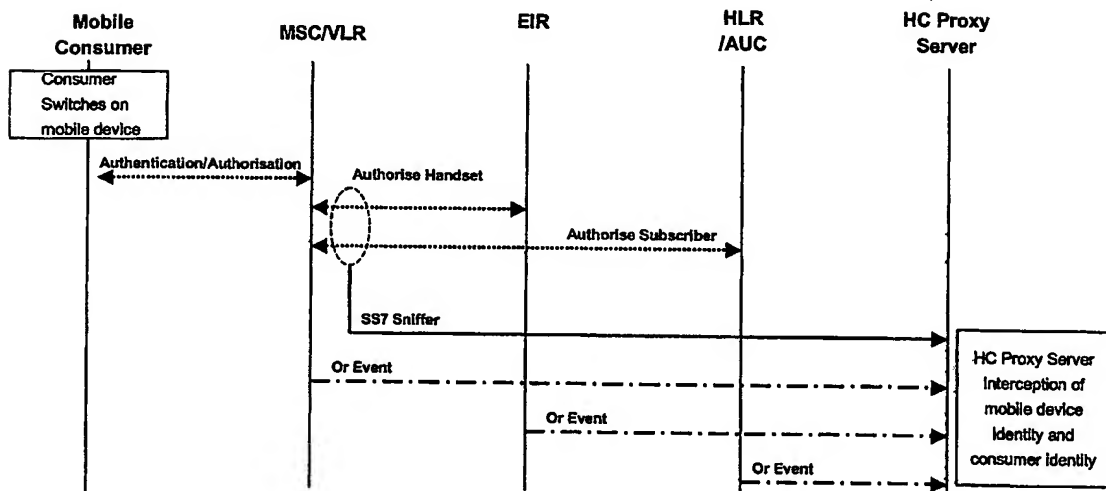


Fig. 4

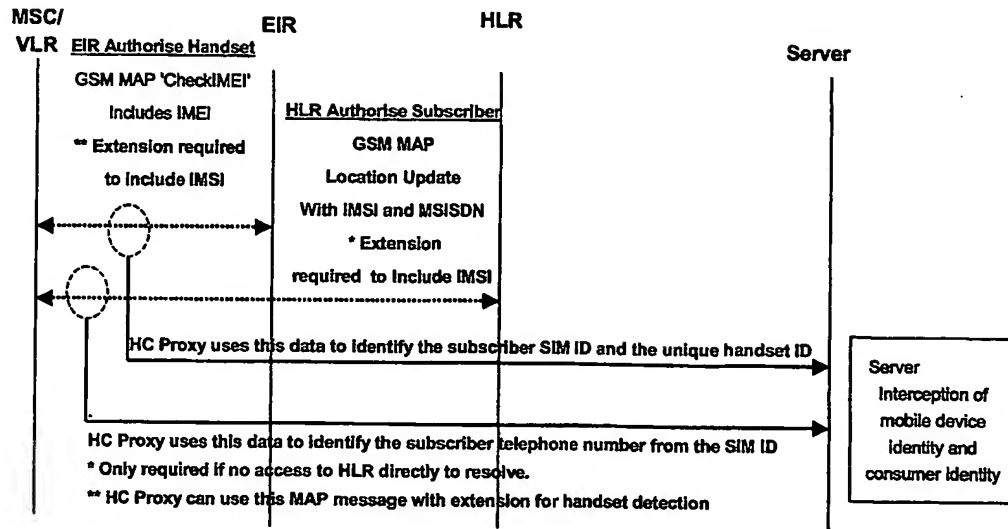


Fig. 5

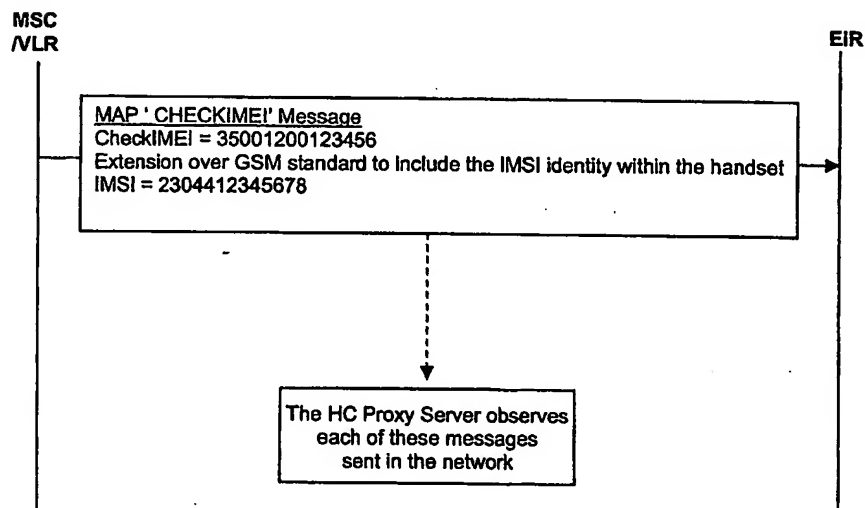


Fig. 6

4/8

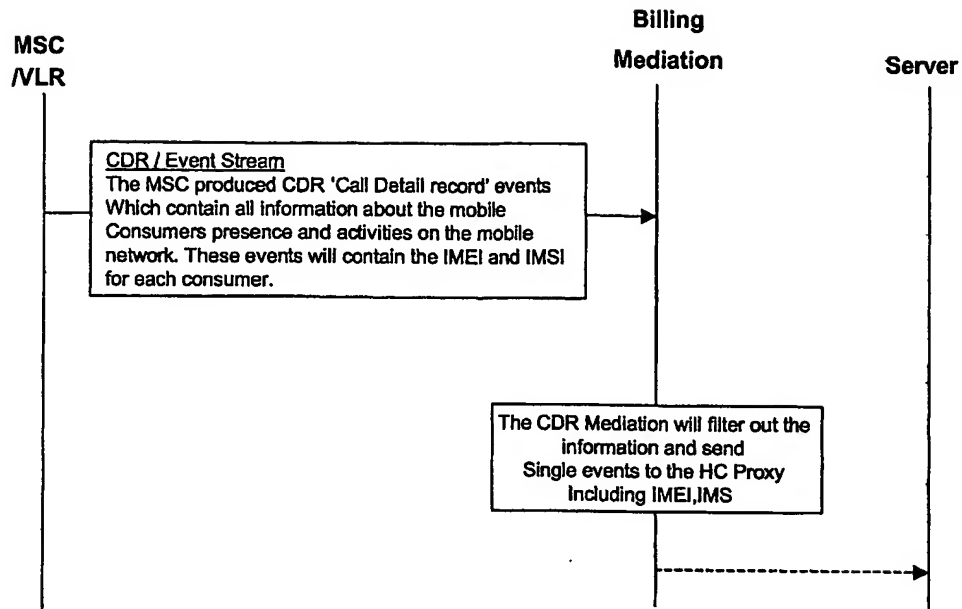


Fig. 7

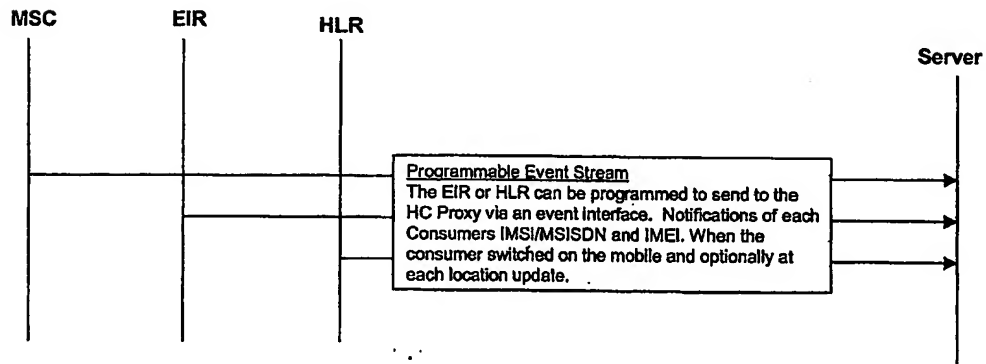


Fig. 8

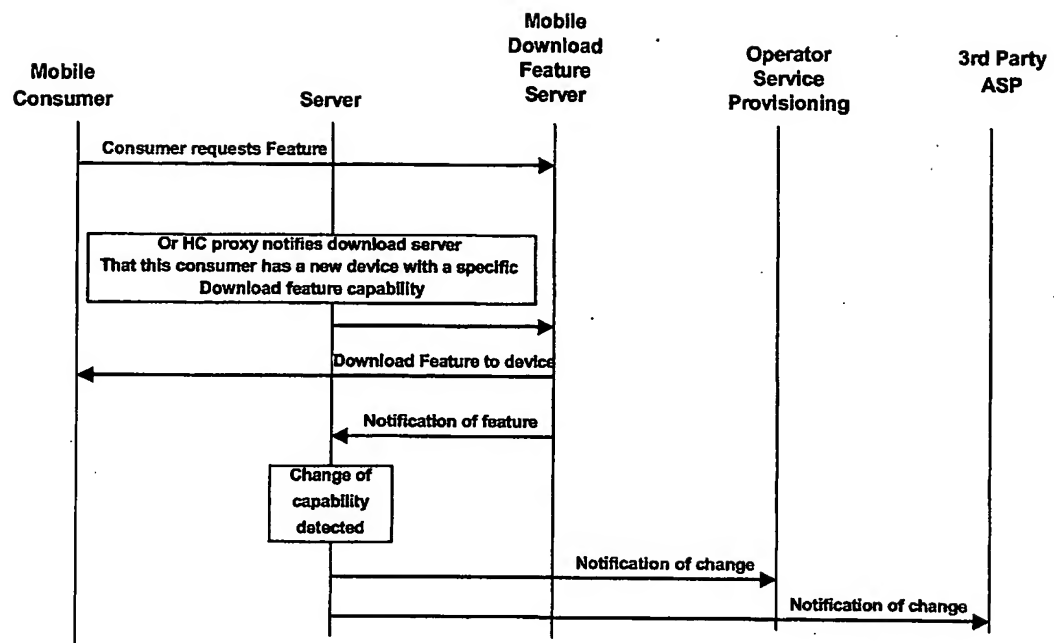


Fig. 9

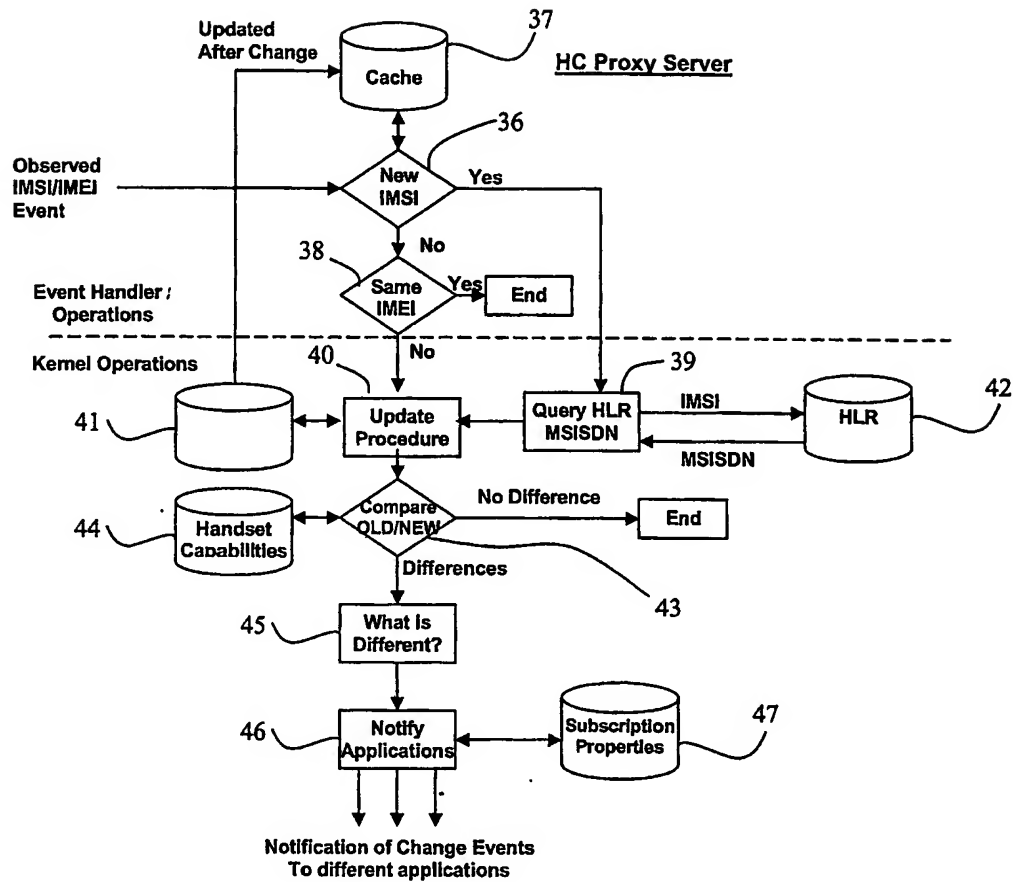


Fig. 10

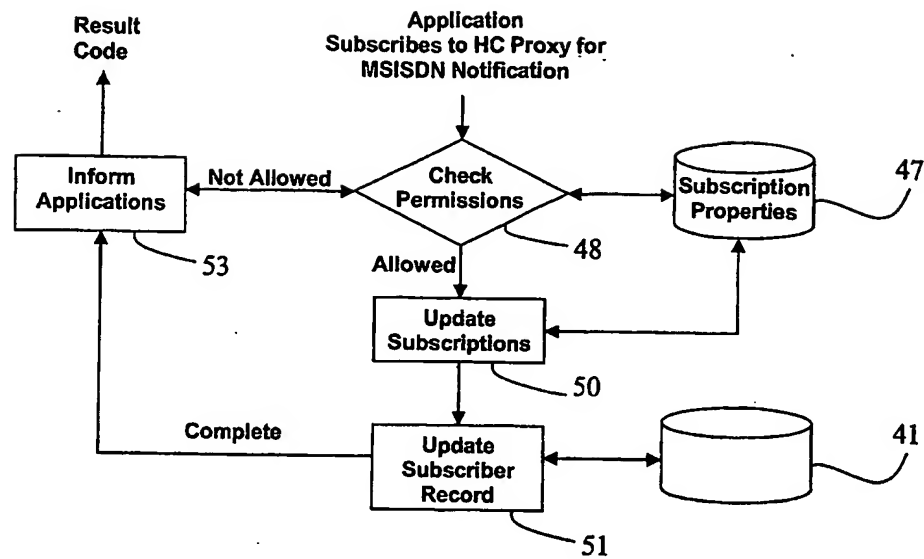


Fig. 11

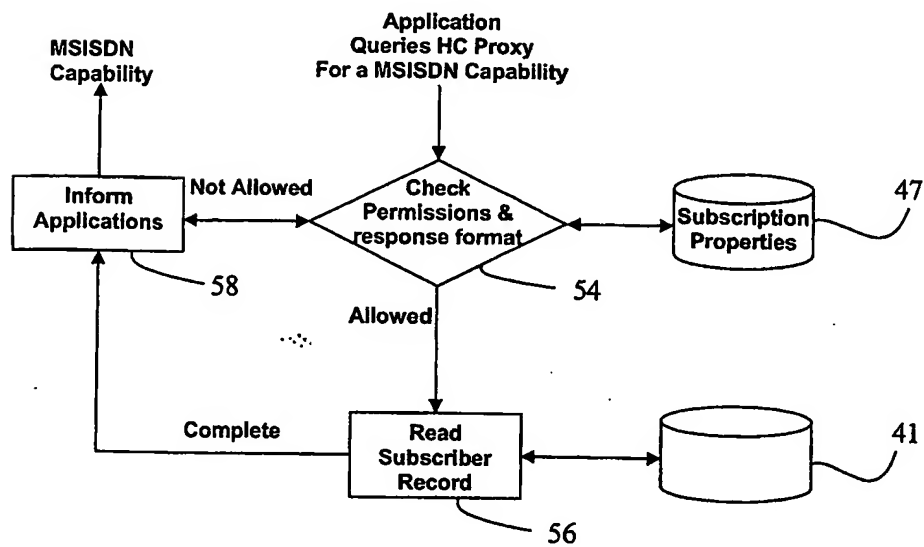


Fig. 12

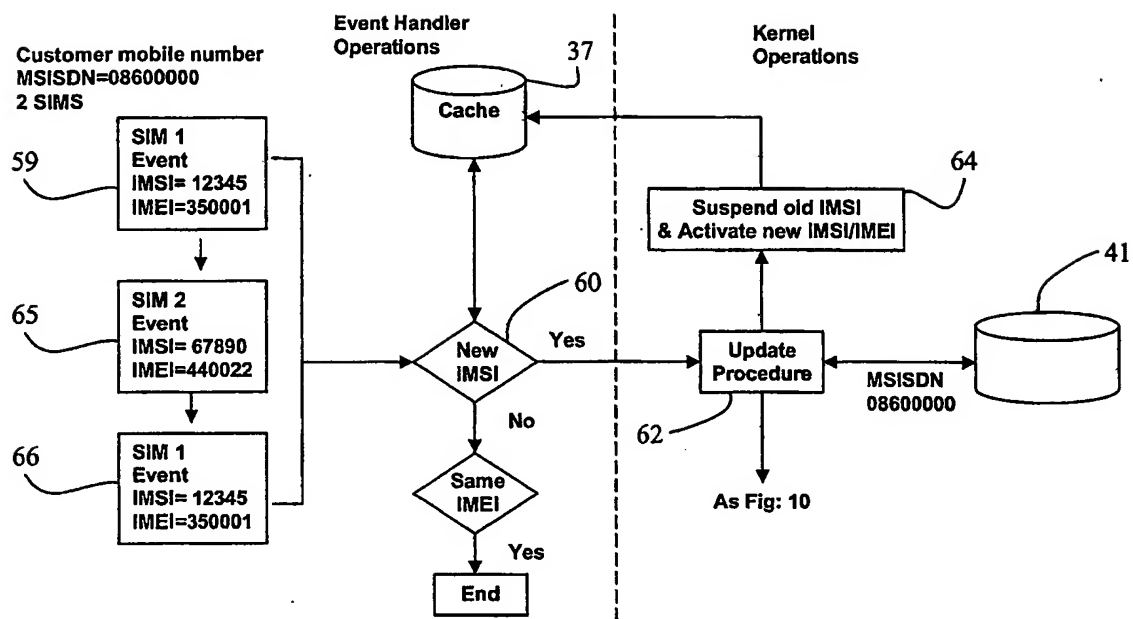


Fig. 13

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/IE2004/000108

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 H04Q7/34

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X  A	<p>WO 02/095529 A (EVOLVING SYSTEMS INC) 28 November 2002 (2002-11-28)</p> <p>abstract</p> <p>figures 1-4 page 2, line 10 - page 3, line 6 page 4, lines 25-33 page 5, line 10 - page 6, line 11 page 6, lines 25-29 page 8, line 31 - page 9, line 19</p> <p style="text-align: center;">----- -/--</p>	<p>1-3, 5-10, 19, 27-30 4, 11-18, 20-26</p>



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*G\* document member of the same patent family

Date of the actual completion of the international search

9 November 2004

Date of mailing of the international search report

23/11/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Mö11, H-P

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/IE2004/000108

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/78425 A (TELECOMM SYSTEMS INC) 18 October 2001 (2001-10-18)	1-3, 8-10, 19, 27-30
A	abstract	4-7, 11-18, 20-26
	figures 1,2,2a page 8, line 12 - page 11, line 4 page 13, lines 1-9	
A	US 2002/022453 A1 (BALOG HORIA ET AL) 21 February 2002 (2002-02-21) paragraphs '0023!, '0029!, '0030!; figure 2 paragraphs '0036! - '0038!; figure 5	18,24
T	"iDec - the IMEI Detection System for consistent MMS quality" POLYSTAR INSTRUMENTS, 'Online! pages 1-7, XP002304482 FARSTA, SWEDEN Retrieved from the Internet: URL:http://www.polystar.com/upload/Polystar_Instruments/Partner/Polystar/Datasheets/iDec_Marketingfolder_1.0.pdf> 'retrieved on 2004-11-04! the whole document	1
T	"Equipment Profile Register - Enable intelligent multimedia content download" STRATUS TECHNOLOGIES TELECOM SOLUTION, PRIME CREATION TECHNOLOGY LTD., 'Online! 2004, pages 1-2, XP002304483 Retrieved from the Internet: URL:http://www.stratus.com/resources/equipmentprofileregister.pdf> 'retrieved on 2004-11-04! the whole document	1

## FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box II.2

Claims Nos.: 31

Claim 31 relies on reference to the drawings and does therefore not meet the requirements of Article 6 PCT and Rule 6.2 (a) PCT.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IE2004/000108

## Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 31  
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:  
see FURTHER INFORMATION sheet PCT/ISA/210
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IE2004/000108

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 02095529	A	28-11-2002	WO 02095529 A2	28-11-2002
			US 2002187781 A1	12-12-2002
WO 0178425	A	18-10-2001	AU 4995101 A	23-10-2001
			WO 0178425 A1	18-10-2001
			US 2001031641 A1	18-10-2001
US 2002022453	A1	21-02-2002	AU 4219601 A	15-10-2001
			WO 0176170 A2	11-10-2001

**THIS PAGE BLANK (USPTO)**